Configurar regras de acesso em um roteador RV34x Series

Objetivo

O roteador VPN de WAN dupla RV340 é um dispositivo flexível, fácil de usar e de alto desempenho, bem adequado para pequenas empresas. Com recursos de segurança adicionais, como filtragem da Web, controle de aplicativos e proteção de origem de IP. O novo RV340 oferece conectividade com fio, banda larga e altamente segura para pequenos escritórios e funcionários remotos. Esses novos recursos de segurança também facilitam o ajuste da atividade permitida na rede.

As regras ou políticas de acesso no RV34x Series Router permitem que a configuração de regras aumente a segurança na rede. Uma combinação de regras e uma ACL (Access Control List, lista de controle de acesso). As ACLs são listas que bloqueiam ou permitem que o tráfego seja enviado de e para determinados usuários. As regras de acesso podem ser configuradas para estarem em vigor o tempo todo ou com base nos agendamentos definidos.

As ACLs têm um deny implícito no final da lista, portanto, a menos que você o permita explicitamente, o tráfego não pode passar. Por exemplo, se você quiser permitir que todos os usuários acessem uma rede através do roteador, exceto endereços específicos, você precisará negar os endereços específicos e permitir todos os outros.

O objetivo deste artigo é mostrar a você como configurar regras de acesso em um RV34x Series Router.

Dispositivos aplicáveis

Série RV34x

Versão de software

- 1.0.1.16
 - <u>Um firmware que atualiza a IU tornou-se disponível desde a publicação deste artigo.</u>
 <u>Clique aqui para ir para a página de downloads e localizar o produto específico ali.</u>

Configurar uma regra de acesso em um roteador RV34x Series

Criar uma regra de acesso

Etapa 1. Efetue login no utilitário baseado na Web do roteador e escolha **Firewall > Access Rules**.



Etapa 2. Na tabela Regras de acesso IPv4 ou IPv6, clique em **Adicionar** para criar uma nova regra.

Note: No RV34x Series Router, é possível configurar até 202 regras. Neste exemplo, IPv4 é usado.

A	Access Rules						
	IPv	4 Access I	Rules Tab	ole			
		Priority	Enable	Action	Service		
		201	\checkmark	Allowed	IPv4: All Traffic		
		202	\checkmark	Denied	IPv4: All Traffic		
		Add	E	dit	Delete		

Etapa 3. Marque a caixa de seleção Enable Rule Status para ativar a regra.

Rule Status:



Etapa 4. No menu suspenso Ação, escolha se a diretiva permitirá ou negará os dados.

Note: Neste exemplo, Permitir é escolhido.



Etapa 5. No menu suspenso Serviços, escolha o tipo de tráfego que o roteador permitirá ou

negará.

Note: Para este exemplo, Todo o tráfego é escolhido. Todo o tráfego será permitido.

Services:	IPv4 IPv	✓ All Traffic
Log:	True 🛟	BGP DNS-TCP
Source Interface:	WAN1 \$	DNS-UDP
· · · ·	· · · ·	COF FTD

Etapa 6. No menu suspenso Log, escolha uma opção para determinar se o roteador registrará o tráfego permitido ou negado. As opções são:

- Nunca O roteador nunca registrará nenhum tráfego permitido e negado.
- Verdadeiro O roteador registrará o tráfego que corresponde à política.

Note: Neste exemplo, Nunca é escolhido.



Passo 7. No menu suspenso Interface de origem, escolha uma interface para o tráfego de entrada ou de entrada onde a política de acesso deve ser aplicada. As opções são

- WAN1 A política se aplica somente ao tráfego da WAN1.
- WAN2 A política se aplica somente ao tráfego da WAN2.
- USB1 A política se aplica somente ao tráfego de USB1.
- USB2 A política se aplica somente ao tráfego do USB2.
- VLAN1 A política se aplica somente à VLAN1 de tráfego.
- Qualquer A política se aplica a qualquer interface.

Note: Se uma VLAN (Virtual Local Area Network, Rede local virtual) adicional tiver sido configurada, a opção de VLAN aparecerá na lista. Neste exemplo, a WAN1 é escolhida.

Source Interface:	✓ WAN1	÷
	WAN2	_
Source Address:	USB1	₽
Destination Interface	USB2	
Doolination monado	VLAN1	P
Destination Address:	Any	\$

política. As opções são:

- Qualquer A política será aplicada a qualquer endereço IP na rede. Se isso for escolhido, vá para a <u>Etapa 12</u>.
- IP único A política se aplica a um único host ou endereço IP. Se isso for escolhido, vá para a <u>Etapa 9</u>.
- Intervalo de IPs A política se aplica a um conjunto ou intervalo de endereços IP. Se isso for escolhido, vá para a <u>Etapa 10</u>.
- Sub-rede A política se aplica a uma sub-rede inteira. Se isso for escolhido, vá para a <u>Etapa 11</u>.

Note: Neste exemplo, Qualquer é escolhido.

Source Address:	✔ Any	Ð
Destination Interface:	Single IP IP Range	÷
Destination Address:	Subnet	•

<u>Etapa 9.</u> (Opcional) O IP único foi escolhido na Etapa 8, insira um único endereço IP para a política a ser aplicada e vá para a <u>Etapa 12</u>.

Note: Para este exemplo, 200.200.22.52 é usado.

Source Address:	Single IP	\$ 200.200.22.52	
· · · · · · · · · · · · · · · · · · ·			

Etapa 10. (Opcional) Se o Intervalo de IPs tiver sido escolhido na Etapa 8, insira os endereços IP inicial e final nos respectivos campos de endereço IP.

Note: Neste exemplo, 200.200.22.22 é usado como o endereço IP inicial e 200.200.22.34 como o endereço IP final.

	Source Address:	IP Range	\$	200.200.22.22	То	200.200.22.34
--	-----------------	----------	----	---------------	----	---------------

<u>Etapa 11.</u> (Opcional) Se a sub-rede tiver sido escolhida na Etapa 8, insira a ID da rede e sua respectiva máscara de sub-rede para aplicar a política.

Note: Neste exemplo, 200.200.22.1 é usado como o ID da sub-rede e 24 como a máscara de sub-rede.

Source Address:	Subnet		200.200.22.1	1	24
		_			

Etapa 12. No menu suspenso Interface de destino, escolha uma interface para o tráfego de saída ou de saída onde a política de acesso deve ser aplicada. As opções são WAN1, WAN2, USB1, USB2, VLAN1 e Any.

Note: Para este exemplo, a WAN1 é escolhida.

Destination Interface	✓ WAN1	
	WAN2	
Destination Address:	USB1	Ð.
	USB2	
	VLAN1	
	Any	
Scheduling		

Etapa 13. No menu suspenso Endereço de destino, escolha um destino para aplicar a política. As opções são Any (Qualquer), Single IP (IP único), IP Range (Intervalo de IP), Subnet (Sub-rede).

Note: Neste exemplo, Qualquer é escolhido. Vá para a Etapa 17.



Etapa 14. (Opcional) Se o IP único foi escolhido na Etapa 13, insira um único endereço IP para a política a ser aplicada.

Note: Para este exemplo, 210.200.22.52 é usado.

Destination Address:	Single IP	\$ 210.200.22.52

Etapa 15. (Opcional) Se o Intervalo de IPs foi escolhido na Etapa 13, insira os endereços IP inicial e final nos respectivos campos de endereço IP.

Note: Neste exemplo, 210.200.27.22 é usado como o endereço IP inicial e 210.200.27.34 como o endereço IP final. Vá para a <u>Etapa 17</u>.

Destinction Address: ID Dane				
Destination Address: IP Rang	le 🗘	210.200.27.22	То	210.200.27.34

Etapa 16. (Opcional) Se a Sub-rede foi escolhida na Etapa 13, insira o endereço de rede e sua respectiva máscara de sub-rede para aplicar a política.

Note: Neste exemplo, 210.200.27.1 é usado como o endereço de sub-rede e 24 como a máscara de sub-rede.

Destination Address:	Subnet		210.200.27.1	1	24
		_	· · · · · · · · · · · · · · · · · · ·		

<u>Etapa 17.</u> Na lista suspensa Nome da programação, escolha uma programação para aplicar essa política. Para saber como configurar uma agenda, clique <u>aqui</u>.



Etapa 18. Clique em Apply.

Access Rules	
Rule Status:	Enable
Action:	Allow \$
Services:	IPv4 IPv6 All Traffic
Log:	True 💠
Source Interface:	WAN1 \$
Source Address:	Any \$
Destination Interface:	WAN1 \$
Destination Address:	Any 🗘
Scheduling	
Schedule Name:	BUSINESS Click here to configure the schedules
Apply Can	cel

Agora, você deve ter criado com êxito uma regra de acesso em um RV Series Router.

Editar uma regra de acesso

Etapa 1. Na Tabela de regras de acesso IPv4 ou IPv6, marque a caixa de seleção ao lado da regra de acesso que deseja configurar.

Note: Neste exemplo, na Tabela de regras de acesso IPv4, a prioridade 1 é escolhida.

IPv	IPv4 Access Rules Table											
	Priority	Enable	Action	Service	Source Interface							
\bigcirc	1	\checkmark	Allowed	IPv4: All Traffic	WAN1							
	2	\checkmark	Denied	IPv4: BGP	WAN1							
	3	\checkmark	Allowed	IPv4: FTP	WAN1							
	201	\checkmark	Allowed	IPv4: All Traffic	VLAN							
	202	\checkmark	Denied	IPv4: All Traffic	WAN							
	Add	E	dit	Delete								

Etapa 2. Clique em Editar.

IPv	IPv4 Access Rules Table										
	Priority	Enable	Action	Service	Source Interface						
	1	\checkmark	Allowed	IPv4: All Traffic	WAN1						
	2	\checkmark	Denied	IPv4: BGP	WAN1						
	3	\checkmark	Allowed	IPv4: FTP	WAN1						
	201	\checkmark	Allowed	IPv4: All Traffic	VLAN						
	202	\checkmark	Denied	IPv4: All Traffic	WAN						
	Add	E	dit	Delete							

Etapa 3. (Opcional) Na coluna Configurar, clique no botão **Editar** na linha da regra de acesso desejada.

Schedule	Configure	Э		
BUSINESS	Edit	Delete	Up	Down
BUSINESS	Edit	Delete	Up	Down
ANYTIME	Edit	Delete	Up	Down
ANYTIME	Edit	Delete	Up	Down
ANYTIME	Edit	Delete	Up	Down

Etapa 4. Atualize os parâmetros necessários.

Access Rules	
Rule Status:	Enable
Action:	Allow \$
Services:	IPv4 IPv6 All Traffic
Log:	True 💠
Source Interface:	WAN1 \$
Source Address:	Any 🗘
Destination Interface:	USB1 \$
Destination Address:	Single IP \$ 192.168.1.1
Scheduling	
Schedule Name:	BUSINESS Click here to configure the schedules
Apply Can	cel

Etapa 5. Clique em Apply.

Access Rules	
Rule Status:	Enable
Action:	Allow \$
Services:	IPv4 IPv6 All Traffic
Log:	True 💠
Source Interface:	WAN1 🗘
Source Address:	Any 🗘
Destination Interface:	USB1 ¢
Destination Address:	Single IP \$ 192.168.1.1
Scheduling	
Schedule Name:	BUSINESS Click here to configure the schedules
Apply Can	cel

Etapa 6. (Opcional) Para alterar a prioridade de uma regra de acesso na coluna Configurar, clique no botão **Acima** ou **Abaixo** da regra de acesso que deseja mover.

Note: Quando uma regra de acesso é movida para cima ou para baixo, ela se move um passo acima ou abaixo de seu posicionamento original. Neste exemplo, a prioridade 1 será movida para baixo.

IPv	Pv4 Access Rules Table												
	Priority	Enable	Action	Service	Source Interf	Source	Destinat	Destination	Schedule	Configure			
	1		Allowed	IPv4: All T	WAN1	Any	USB1	192.168.1.1	BUSINESS	Edit De	elete Up	Down	
	2	V	Denied	IPv4: BGP	WAN1	Any	WAN1	Any	BUSINESS	Edit De	elete Up	Down	
	3	1	Allowed	IPv4: FTP	WAN1	Any	USB2	Any	ANYTIME	Edit De	elete Up	Down	
0	201		Allowed	IPv4: All T	VLAN	Any	WAN	Any	ANYTIME			Down	
\bigcirc	202	\checkmark	Denied	IPv4: All T	WAN	Any	VLAN	Any	ANYTIME	Edit De		Down	
	Add	6		Delete									

Note: Neste exemplo, a prioridade 1 agora é prioridade 2.

IP	IPv4 Access Rules Table												
	Priority	Enable	Action	Service	Source Inter	Source	Destina	Destination	Schedule	Configure			
	1	V	Denied	IPv4: BGP	WAN1	Any	WAN1	Any	BUSINESS	Edit	Delete	Up	Down
\square	2	V	Allowed	IPv4: All Tr	WAN1	Any	USB1	192.168.1.1	BUSINESS	Edit	Delete	Up	Down
0	3	V	Allowed	IPv4: FTP	WAN1	Any	USB2	Any	ANYTIME	Edit	Delete	Up	Down
	201	V	Allowed	IPv4: All Tr	VLAN	Any	WAN	Any	ANYTIME	Edit	Delete		Down
\bigcirc	202	V	Denied	IPv4: All Tr	WAN	Any	VLAN	Any	ANYTIME	Edit	Delete		Down
	Add	E	dit										

ly.
ly

IP	4 Access	Rules Tab	ole								
	Priority	Enable	Action	Service	Source In						
	1	\checkmark	Denied	IPv4: BGP	WAN1						
	2	\checkmark	Allowed	IPv4: All Traffic	WAN1						
	3	\checkmark	Allowed	IPv4: FTP	WAN1						
	201	\checkmark	Allowed	IPv4: All Traffic	VLAN						
	202	\checkmark	Denied	IPv4: All Traffic	WAN						
	Add) [E	dit	Delete							
IPut Access Pules Table											
IPv	6 Access	Rules Tab	le								
IPv	6 Access Priority	Rules Tab Enable	Action	Service	Source In						
	Priority 201	Rules Tab Enable	Action Allowed	Service IPv6: All Traffic	Source In VLAN						
	Priority 201 202	Rules Tab Enable	Action Allowed Denied	Service IPv6: All Traffic IPv6: All Traffic	Source In VLAN WAN						

Você deve ter editado com êxito uma regra de acesso em um RV34x Series Router.

Excluir uma regra de acesso

Etapa 1. Na Tabela de regras de acesso IPv4 ou IPv6, marque a caixa de seleção ao lado da regra de acesso que deseja excluir.

Note: Neste exemplo, na Tabela de regras de acesso IPv4, a prioridade 1 é escolhida.

IPv	IPv4 Access Rules Table											
	Priority	Enable	Action	Service	Source Interface							
	1	\checkmark	Allowed	IPv4: All Traffic	WAN1							
	2	\checkmark	Denied	IPv4: BGP	WAN1							
	3	\checkmark	Allowed	IPv4: FTP	WAN1							
	201	\checkmark	Allowed	IPv4: All Traffic	VLAN							
	202	\checkmark	Denied	IPv4: All Traffic	WAN							
	Add	E	dit	Delete								

Etapa 2. Clique em **Excluir** localizado abaixo da tabela ou clique no botão excluir na coluna Configurar.

IPv	IPv4 Access Rules Table										
	Priority	Enable	Action	Service	Source Interface						
	1	\checkmark	Allowed	IPv4: All Traffic	WAN1						
	2	\checkmark	Denied	IPv4: BGP	WAN1						
	3	\checkmark	Allowed	IPv4: FTP	WAN1						
	201	\checkmark	Allowed	IPv4: All Traffic	VLAN						
	202	\checkmark	Denied	IPv4: All Traffic	WAN						
	Add	E	dit	Delete							

Etapa 3. Clique em Apply.

cce	ess Rule	es			
IPv	4 Access	Rules Tab	ole		
	Priority	Enable	Action	Service	Sourc
	1	\checkmark	Denied	IPv4: BGP	WAN
	2	\checkmark	Allowed	IPv4: FTP	WAN1
	201	\checkmark	Allowed	IPv4: All Traffic	VLAN
	202	\checkmark	Denied	IPv4: All Traffic	WAN
	Add	E	dit	Delete	
IPv	6 Access	Rules Tab	le		
	Priority	Enable	Action	Service	Sourc
	201		Allowed	IPv6: All Traffic	VLAN
	202	\checkmark	Denied	IPv6: All Traffic	WAN
	Add	E	dit	Delete	
Ap	oply	Restore t	o Default R	Rules Service Man	agement

Agora você deve ter excluído com êxito uma regra de acesso no RV34x Series Router.

Exibir um vídeo relacionado a este artigo...

Clique aqui para ver outras palestras técnicas da Cisco